YANG Provenance Signatures Integrated with the Kafka Schema Registry

-

IETF Hackathon

IETF 124

1–2 November 2025

Montreal, Canada

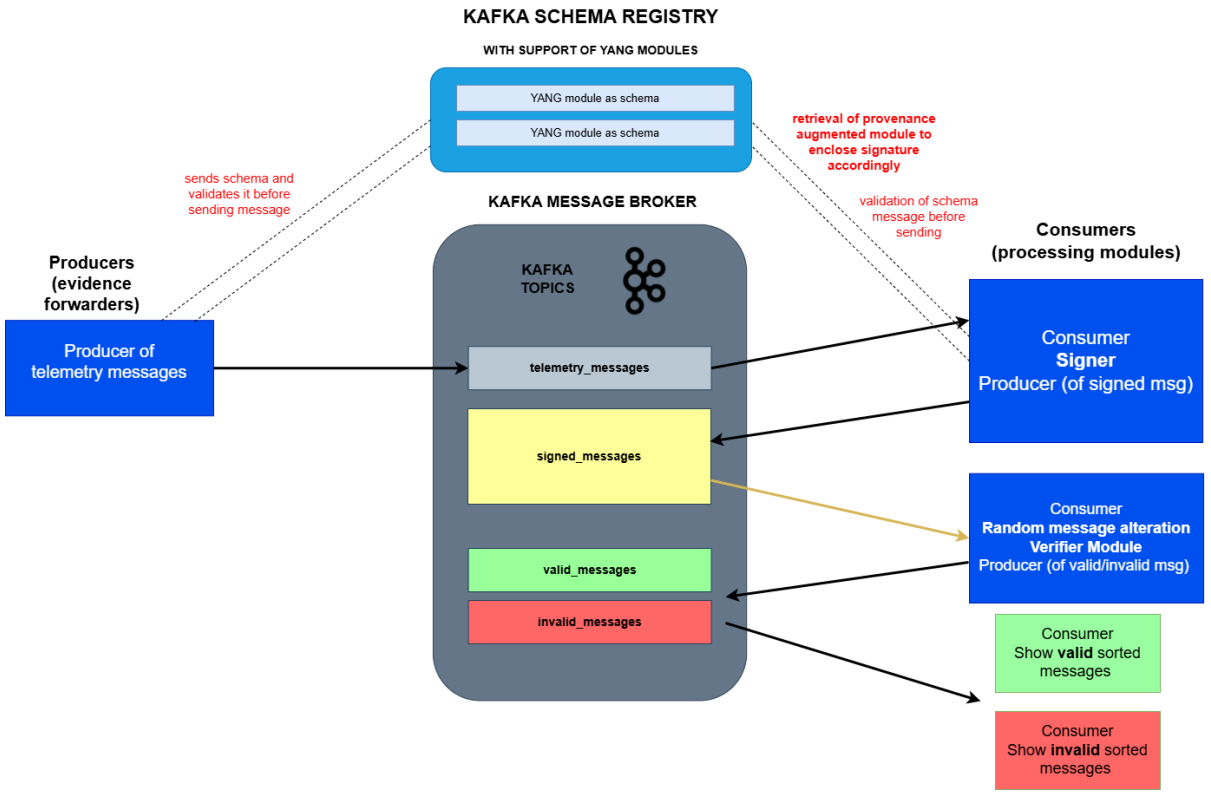
Prov·e·nance | ˈprävən(ə)ns |

- More specifically, *data provenance*
  - A documented trail accounting for the origin of a piece of data and where it has moved from to where it is presently
- Assurance of the origin and integrity of YANG datasets
  - Whenever the dataset is used beyond an original online flow
    - Use of data intermediaries, such as data lakes
    - AI/ML training and validation
    - Audit trails, including forensics evidence
- Initial use cases
  - Device configuration integrity
  - Telemetry and monitoring data source and integrity
  - Network-wide service orchestration assurance
- Procedures defined in draft-ietf-opsawg-yang-provenance

What We Brought

- An enhanced provenance signature library
  - Aligned with the latest version of the draft
  - Enhanced management of module augmentation
  - Enhanced logic to apply YANG schemas to signature procedures
  - Seamlessly integrable with any YANG processing pipeline
- Integrated with Kafka schema registry
  - As defined in draft-ietf-nmop-yang-message-broker-integration
  - Use the Kafka schema registry for guiding the signature procedures
  - Signing and verification become full schema-based

Kafka Integration Details



1. A **producer** sends data to a *telemetry_messages* topic, once its schema its validated with the YANG schema registry

2. A consumer signs the given data according the provenance YANG module augmentation retrieved from the YANG Kafka schema registry, and forwards it to *signed_messages* topic.

3. The **verifier module** consumes from *signed_messages*.

4. This module **randomly** alters some messages to simulate **tampering** and then are cryptographically **verified**.

5. The message is forwarded to *valid_messages* or *invalid_messages* depending on the verification result.

6. Two separate consumers read and display these topics.

What We Achieved Here

- As originally intended
  - Demonstrate RI evolution, aligned with the draft
  - Enhance the Kafka integration demonstrated in IETF123
- Progress in YANG provenance signature and verification
  - Full schema-based signature processing
  - Clean procedure for applying provenance signatures
- Progress in the convergence with YANG Push
  - And Kafka schema registry